Internet of Things - Secured Communications between the host with Cellular Networks using multiple authentication systems

S. B. Bharath, Deepanjali Chandrasekaran and M. S. Minu

March 5, 2020

Internet of Things - Secured Communications between the host with Cellular Networks using multiple authentication systems

Bharath S B
Email: annu0471@gmail.com

Deepanjali Chandrasekaran
Email: deepuchandru2001@gmail.com

Minu M S
Email: msminu1990@gmail.com

***Index Terms*—Internet of things, Authentication, Security**

I. ABSTRACT

This paper aims to provide a solution for secured communication between the hosts and cellular networks using the Internet of Things. This technique works with different layers of security for information transmission between the devices and hence the system creates a highly secured transportation of information between the hosts or the devices.

II. INTRODUCTION

IoT devices are an indispensable part of our life. With the development of the world more and more IoT devices and made to make the working processes faster and efficient. In simple words, IoT devices can be defined as devices that interact with the network in transferring data and also collecting it without the human-human or human-computer involvement. With the evolvement of these devices, there are also pot ential security rises in the devices and also in the safe transfer of data between devices and the host.

Fig. 1. Secured communication between the host

Substandard architecture in the cellular network can disclose security risks. An eminently secured architecture with multilayered security advancement should be implemented to produce a comprehensive design for connection, for safe linkage and transfer of data from the device to the targeted host for processing, storage, and additional uses.

Apart from cellular connection, devices might connect with public Ethernet or Wireless WI-FI networks to freightage the data from edge devices to the host. Connecting these devices consort numerous vulnerabilities. The fractious texture of IoT devices – i.e. Device interacting with the backend host without any human synergy – equip the definition for distant control and tracking of devices. Due to the fractious nature of devices, data transferring cannot be controlled or track steadily.

At present, there are numerous Vulnerabilities in the public networks which can be exploited to get access to IoT devices and manipulate it. Some includes:

* Rogue Access point/Ad-Hoc Networks
* Denial of Service
* Passive Capturing
* problems(Mis-Configuration/Incomplete Configuration)

III. RELATED WORKS

The system architecture consists mainly of two planes i.e. The control plane and User plane. The user plane function (UPF) contains the packet routing, packet forwarding, policy enforcement, branching point to support multi-homed public display unit (PDU) sessions and handling quality of service(QoS).[1]

5G is the upcoming technology for security in IoT device communications. Threat Model considers threats to 5G enabled IoT service. Threat on authentication is a possibility of an unauthenticated attacker who has the capability of monitoring as an authorized user. The threat to confidentiality is an unauthorized person who could access and understand the unauthorized service-query or service-allocation in the path to 5G technologies [1].Threat to integrity: An attacker could monitor the service-request/user-credentials in 5G and user equipment.

According to new technologies our life will be expected to be completely dependent on the IoT devices. T here must be many security layers in the IoT devices to have secured communication between the host

A currently available cryptographic algorithm is used to make sure that the data is communicated between the host with a complete security, which is a very secure algorithm. IoT is focusing on the host to host mode of communication. For such communication, authentications are very important for ensuring security. When two or more nodes are communicating with each other they should have an authentication process between each other first in order to block fake device attacks.[2]

There is some limitation in security aspects for the cluster of networks like devices must have cellular network subscriptions, devices must subscribe with the same network, etc. In a large space, an infrastructure-less network takes more time to find a similar network hence a fixed network is required to overcome the problem. The architecture must provide reliable communication within the clusters[3].

Comparison of inband Device to device communication and outband device to device communication concluded outband device to device communication be the usable alternative. Unlicensed spectrum is used by outband the device to device communication. There is some inband limitation which is comparatively more than the outband limitations[4].

There are some algorithms used for the device to device communication to have better communication: Hierarchical Algorithms , Stochastic Algorithms, Context-Aware Algorithms , Bio-inspired Algorithms.

For the communication process, we must know the route or the pathway to send the information, the route decision system is important for the communication process. Information that is required in the route request is a Source address, a Destination address, Sequence number, etc.[5]. This would help for proper communication between the devices, there will not be any mismatch in data.

Few security features that are currently present are:

* Network access security-User identity confidentiality, Entity authentication, Data integrity, Mobile equipment identification.

*Network domain security.

*User domain security-User-to-USIM authentication, USIM-Terminal Link[7].

The USIM provides security features. some of the security requirements are PIN, PIN-enabled or disabled indicator, PIN error counter, Unblock PIN, Subscriber authentication keys. A Phone Book entry consists of a record in an ADN(Abbreviated Dialing Number) file and additional records that are stored in different elementary files[8]. Storage of call details will be helpful for security purposes during communication.

SIM/USIM personalization cycle-Access to the personalization process would have been restricted for unauthorized, accidental or any unwanted attack. SIM/USIM de-personalization provides a keypad entry.[9]The security features have to maximize the number of the device to device links and reduce the power consumption of the device to device links in the system.[10]

IV. Existing model

In the current technology, there are many security features. The need for secure data communication is increasing instantly. The WAP protocol makes use of network security layers to provide a secure path for communication. Universal Mobile Telecommunications Service Authentication and Key Agreement of (UMTS AKA) mechanism are in charge of providing AKA using the response mechanism.

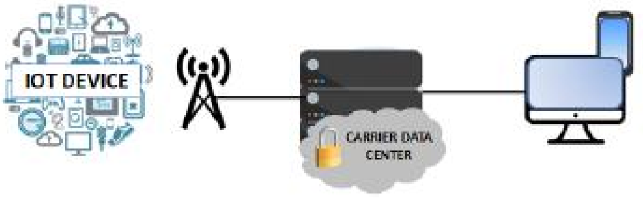

Fig. 2. Architecture System description

Device-to-device communication is mainly implemented for safe communication. The target of D2D communication is for public safety and also for commercial applications. (IMEI) International Mobile Equipment Identity number is a special 15 digit number for GSM phones to identify it. It is one of the methods to track the phone.

Various types of methods for a secured communication which includes:

- PIN locking of SIM.
- Radio access network encryption.
- Private TCP/IP Addressing.
- Data transmission between the host and the Device.
- Implied device to device communication.
- IMEI authentication.
- USIM - Universal subscriber identity module.

The new technologies are emerging the attackers are also being increased. The attackers use new technologies for hacking information during communication. Tracking of data packets helps to monitor the abnormal behavior of data. APN is access point name, it's a name of a gateway between the mobile network and the computer network. Cellular device have to configure with the APN whenever it makes a data communication. Each and every data packet in the communication has to be monitored to ensure their proper path for their destinatio host.

V. Proposed model

The methodology interpreted here provides a secure wireless connection of packet data and the cellular device establishing a sturdy connection between the device and the host. The perfect security technology can provide stronger protection and more secure access, processing and storage.

Hardware authentication, cloud technology, deep learning makes data communication more secure. With the existing model, the upcoming versions for 4g and 5g technologies can be improved to have highly secured communication between the hosts.

The methodology consists of various types of methods which includes:

- SIM-based authentication and PIN locking of SIM.
- Radio and Custom access network encryption.
- Private non-routable TCP/IP Addressing.

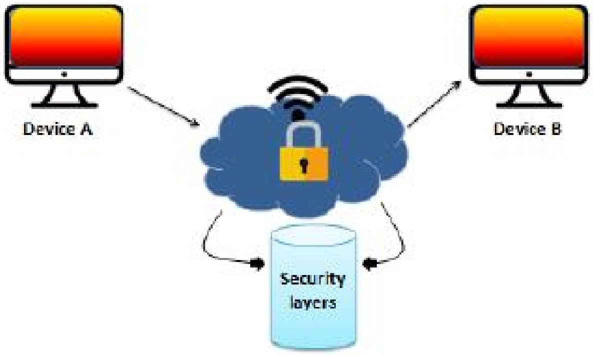

Fig. 3. Security layers between the communication

- non-split tunnel routing schema.
- Data transmission between the host and the Device.
- Implied device to device communication.
- IMEI authentication.
- USIM - Universal subscriber identity module.
- SEAF - Security Anchor Function.
- AUSF - Authentication Server Function.
- UDM - Unified data management.
- SIDF - Subscription Identifier De-concealing Function.

VI. Cellular network Description

Cellular networks are high-speed, high-capacity data communication networks that consists of a base station and a host, by which the data is transmitted through an encrypted radio access network.

The Advantage of this Architecture is that it provides:

1. Connection between fixed and wireless cellular users.
2. It is easy to maintain and upgrade.
3. It uses less transmission power.

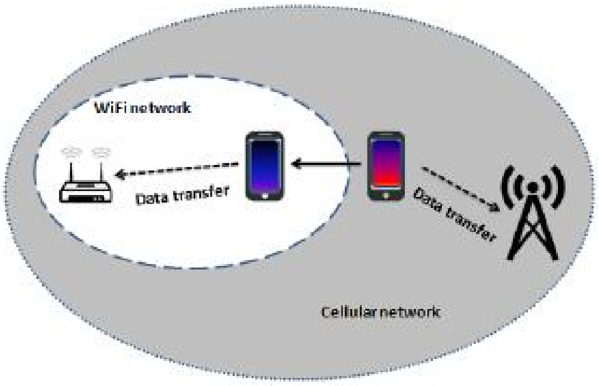

Fig. 4. The above diagram shows the cellular network description

VII. Interlinking of authentication techniques

Each layer of the different authentication processes is included in the complete architecture of the system for the secured data transmission. Each layer has been briefly explained in this section:

A) SIM-base d authentication and PIN locking of SIM

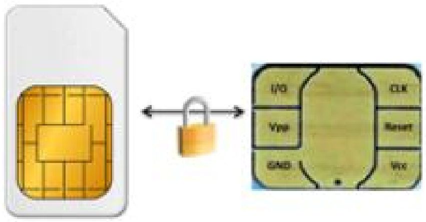

Fig. 5. PIN locking of SIM

This method provides an additional layer of protection to the device. SIM is made of a microprocessor that prevents the compromisation of authentication keys. A SIM consists of a pin unlock key(PUK). This pin is used by the service providers to restrict the use of their network in some countries. This can also be called as SIM lock, network lock or carrier lock. The connection of the SIM is through the radio module.

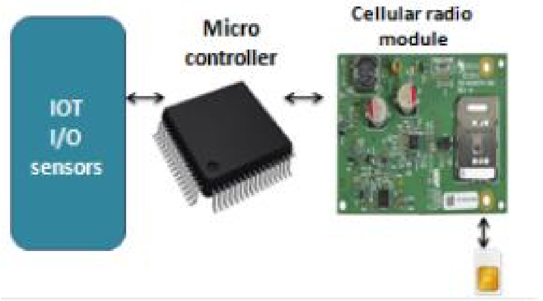

Fig. 6. IoT cellular wireless device

B)Radio and Custom access network encryption.

The gateway between the Device and the cellular network which is configured by the carrier to provide an IP Address is known as Random Access network. Cellular companies can produce their own custom APN's. The APN provides an extra layer of security to the IoT device by not excepting the Malicious file by ending the section.

C) Private non-routable TCP/IP Addressing

An internal security layer used to provide a dynamic IP Address to the cellular Device from a range of reserved IP scopes to protect the device from malicious data. However, if a malicious file is passed to the network tunnel, the Custom APN's drops the packets. It is not such that the routable Addressing does not provide an internet connection between

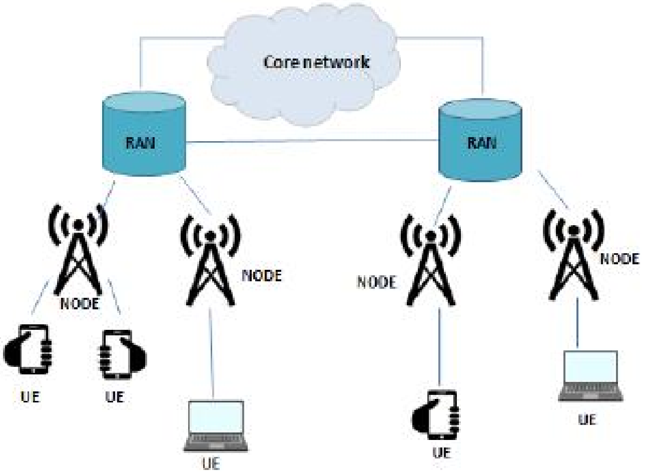

Fig. 7. Radio access network

the device and the Host, while it provides an Extra Firewall to the device by not letting all the data to pass through it.

D) Data communication between the host an d the Device

The data transmission between the host and the Device can take place through IPsec VPN tunnel, MPLS, frame relay or through Multiple landline connectivity. Most of the IPsec VPNs commonly use the Cisco VPN firewall at both devices and the host ends. With the Combination of IPsec VPN and APN is would be easy to validate a secured path between the host and the device for the communication.

E) Implied device to device communication

This paper avoids direct communication between the devices instead of IoT devices are been included between the devices for secured communication. The information is carried from machine A to IoT device and from that device, the information is carried to another IoT device which is connected with machine B.

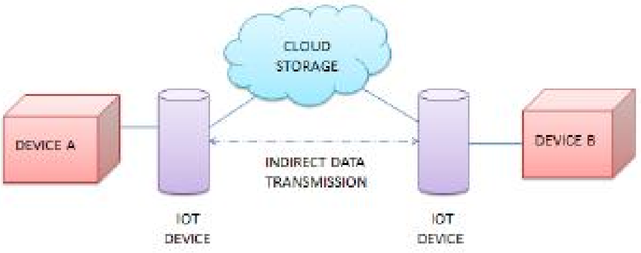

Fig. 8. Indirect Data Transfer

An IoT device has been used the information is transferred in a secure manner between the devices. In this IoT devices will be providing main authentication layers such as:

- Application layer
- support layer
- Perceptual layer
- Network layer

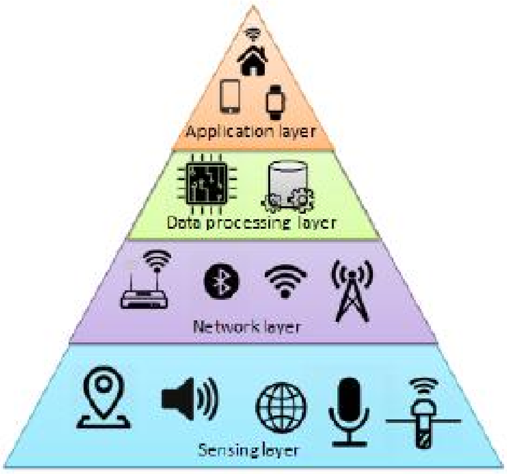

Fig. 9. Architecture of IoT

F) IMEI – international mobile equipment identity

IMEI number is used by cellular networks to identify valid devices. As a unified identification number, it contains information on the device manufacturer, brand, model, and specifications, and ensures device authenticity. It contains 15 decimal digits, 14 digits and 1 check digit or IMEISV which contains 16 decimal digits number, 14 digits and two software version digits which contains the information on the origin, model, and the serial number of the device.

G) USIM - Universal subscriber identity module

USIM or SIM card is a card used by mobile phones to stores card holder's information in an encrypted manner. It is a telecommunication algorithm through which they can communicate securely. One of the key security features of GSM, UMTS and LTE is the concept of the SIM. This card allows the user to keep his/her identity while transferring or upgrading phones. The universal subscriber identity module (USIM) is one of several software applications that resides in the hardware part, called the universal integrated circuit card (UICC).

H) SEAF - Security Anchor Function

The Security Anchor Function (SEAF) is in a serving network. It works as an intermediate between the user equipment and the home network during the authentication process. It can deny an authentication request from the Equipment, but it depends on the user equipment home network to accept the authentication.

I) AUSF - Authentication Server Function

The Authentication Server Function (AUSF) is in a home network. It implements an authentication process with a User Equipment. It decides on User Equipment authentication, but it depends on backend service for computing the authentication data and keying materials when 5G EAP- Authentication key agreement ' is used. Subscriber authentication, during the certification of 5G, is managed by the Authentication Server

Function (AUSF), which access authentication vectors from the UDM.

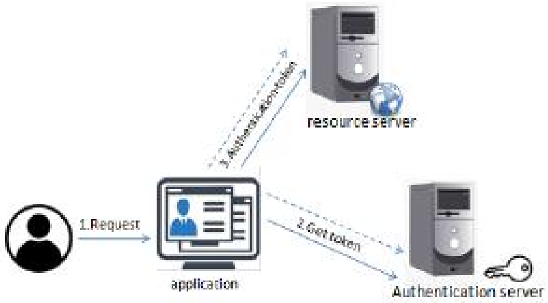

Fig. 10. Authentication Server

J) UDM - Unified data management

Unified data management (UDM) is an entity that hosts functions related to data management, such as the Authentication Credential Repository and Processing Function (ARPF), which selects an authentication method based on subscriber identity and configured policy and computes the authentication data and keying materials for the AUSF if needed. Unified data management (UDM) manages network user data in a single, centralized element. UDM is similar to the 4G network's home subscriber service (HSS) but is cloud-native and designed for 5G specifically.

L) SIDF - Subscription Identifier De-concealing Function

The Subscription Identifier De-concealing Function (SIDF) decodes a Subscription Concealed Identifier (SUCI) to obtain its indelible identity, namely the Subscription Permanent Identifier (SUPI). In 5G, a subscriber indelible identity is always transferred over the radio interfaces in a secured form. Public key-based encryption is used to protect the SUPI. Therefore, only the SIDF has access to the private key associated with a public key distributed to UEs for encrypting their SUPIs. The SIDF is a functional element of the UDM (Unifi ed Data Management), used for decrypting and SUCI (Subscription Concealed Identifier) to reveal the subscriber's SUPI (Subscription Permanent Identifier).

VIII. Conclusion

This paper provides a solution for secured communication between the hosts using the Internet of Things with cellular networks.

Mobile users, internet users, and mobile social media users have been increasing with the increase in years. The plotted graph shows as technology increases the crime is been also increased. So we need to increase the security parallelly with the increase of cybercrime.

This technique contains many layers of authentication process which includes upcoming 5G authentications for secured data transmission. The system architecture will provide reliable communication within and between the hosts.

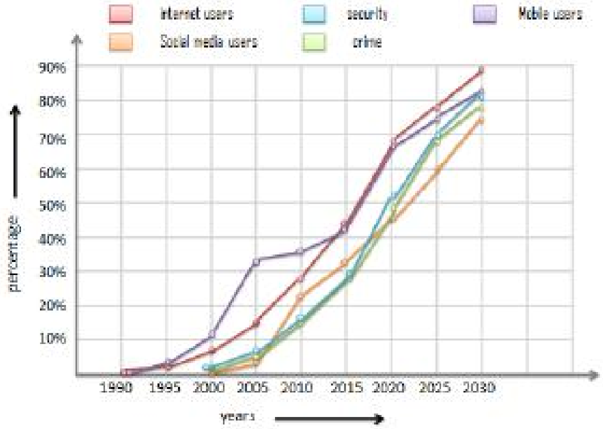

Fig. 11. current usage of technology

IX. REFERENCES

[1] Secure Authentication Protocol for 5G Enabled IoT Network Suraj Sharma1, Shaswat Satapathy1, Shivani Singh1, Amiya Kumar Sahu1, Mohammad S. Obaidat, International Institute of Information Technology, Bhubaneswar, India, 5th IEEE International Conference on Parallel, Distributed and Grid Computing(PDGC-2018), 20-22 Dec 2018, Solan, India

[2] Internet of Things Security, Device Authentication and Access Control: A Review, Inayat Ali*1, Sonia Sabir1, Zahid Ullah2, International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 8, August 2016

[3] A Composite Model for an Intelligent Device-To-Device Communication in the Internet of Things, B. Kalpana, R. Sanjay, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-1S, November 2019

[4] Review on Device-to-Device Communication, Ankita Singha, Sona Sharma, International Jou rnal of Engineering Technology Science and Research IJETSR www.ijetsr.com ISSN 2394 – 3386 Volume 4, Issue 5 May 2017.

[5] A Generic Framework for Context-Aware Routing and its Implementation in Wireless Sensor Networks, Bernd-Ludwig Wenning, Andreas Timm- Giel, Carmelita Görg Communication Networks, University of Bremen, Germany.

[6]A Survey of Internet of Things (IoT) Authentication Schemes †

Mohammed El-hajj 1,2, Ahmad Fadlallah 1, Maroun Chamoun 2 and AhmedSerhrouchni3, The first one is: In Proceedings of the 2017 1st Cyber Security in Networking Conference (CSNet), Rio de Janeiro, Brazil, 18–20 October 2017; pp. 1–3 and the second one is: In Proceedings of the 2017 IEEE 15th Student Conference on Research and Development (SCOReD), Putrajaya, Malaysia, 13– 14 December 2017; pp. 67–71.

[7]3GPP TS 33.102 V3.11.0 (2002-03),3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; SecurityArchitecture

[8]3GPP TS 21.111 V12.0.0 (2014-10),3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; USIM and IC card requirements

[9]3GPP TS 22.022 V12.0.0 (2014-10) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Personalisation of Mobile Equipment (ME); Mobile functionality specification

[10]A Novel Access Control and Energy-Saving Resource Allocation Scheme for D2D Communication in 5G Networks, Ning Du,1,2 Kaishi Sun,1 Changqing Zhou,3 and Xiyuan Ma4, Hindawi Complexity Volume 2020, Article ID 3696015, 11 pages https://doi.org/10.1155/2020/3696015